Rapid Risk Analysis for Information Security

Panel Discussion

Hilary H. Hosmer, Chair
Data Security, Inc.
58 Wilson Road
Bedford, MA 01730

INTRODUCTION

Information warfare threatens our national information infrastructure, the Year 2000 bug puts legacy systems in jeopardy, and "cookies" and data warehousing threaten our privacy. Unfortunately, the traditional guidelines for INFOSEC risk analysis emphasize time-consuming quantitative measurements that produce misleadingly precise results. Oftentimes, we don't have the time or the resources to do a traditional risk analysis. This panel presents rapid risk analysis alternatives ranging from 15 minutes to two weeks.

PANELISTS

Walter Cooke was part of the Canadian team that set up the election information system for the 1994 election in South Africa, the first universal election. The team, responsible for the disaster recovery portion of the system, took only 15 minutes (!) to do the risk analysis for a large, critical, internationally visible system. As a result of the analysis, the Canadians networked the country in triplicate (cable, microwave, and satellite) and set up multiple back-up sites, both hot and cold, in different parts of the country.

Caroline Hamilton, president of RiskWatch, introduced a two-day risk analysis product to be used by schools. Sales went slowly until the school shootings in Colorado and Georgia. Suddenly schools across the nation wanted automated support for rapid risk analysis.

Whereas many risk analysis products ask for lots and lots of data, Trident's **NETrisk** requires very little user input. A representative from Trident will explain how their expert system greatly speeds up secure network risk analysis and design.

A researcher specializing in risk analysis for the critical information infrastructure will join us from Sandia National Labs.

Hilary Hosmer, panel chair, is president of Data Security, Inc. and founder of the New Security Paradigms Workshop. She led a risk analysis for NASA, surveyed metrics used in risk analysis tools, and wrote a paper on visualizing risk metrics for the Naval Research Laboratory (NRL). She is interested in new paradigms for risk analysis.

Position Statement of Walter Cooke – NISSC Rapid Risk Assessment Panel

The initial situation is hopeless!

- Massive undertaking: 1,219,090 sq. km, 28 million voters (24 million new), 320,000 IEC workers, 14,000 voting stations, no electricity or communications to large areas of the country, 50% unemployment, "Civil war" in progress
- 1st all party, democratic election, with 22? parties running candidates
- Security: no time for a plan, and a "drop dead" deadline: 1 month to go…
- Few experienced staff: most had never voted before, let alone run an election
- Fear and uncertainty: the end of Apartheid is perceived as the end of power for the white minority, bringing an unknowable future
- Voter education is a massive effort to ensure the election is "free and fair"
- Rapid changes in threats, vulnerabilities, safeguards, and attitudes to security over short time span
- Robust security is not "politically expedient" for the Independent Electoral Commission (IEC)

The TRA: What, me worry?

- "15 minute TRA": everything can happen, everything has already happened, everything will probably happen again before we get done
- Assessing the situation: thinking "outside the box" – design for peace, build for war
- A TRA or a DRP? NEITHER is appropriate
- Agency: who can do what, to whom, and with what?
- Ourselves as agents and outside eyes: how can we be as strong as the threat agents?
- Learn from the past: (World Trade Centre bombing)
- Be in the present: (riots, bombings, assassinations, sabotage, strikes)
- Look to the future: ("How would 'I' stop the election?")
- Contingencies and scenarios: how many times has it happened already, and how do we mitigate, or continue onward?
- Ensuring function recovery rather than asset recovery will be the core response to threat actions when safeguards and deterrents do not work

How did we reduce risk (and succeed)?

- If the sky is falling, then "price is no object!"
- Industrial strength security: boost safeguards to same level of strength as threats?

- It is easier to beg forgiveness than to get permission

- Domino theory: stop toppling dominos from hitting other dominos
- Cheque please!: multiple (unlikely) intelligence sources
- The old shell game: multiple redundant distributed resources
- Pressing CD's: multiple redundant backups
- Strength in numbers (320,000 workers; 23 IT staff?)
- Intimidation w/military force: "Stop the trains!"
- Deception and misinformation (distribution of weaknesses)
- Spread responsibilities across multiple agencies
- "Pulse the system" – are the safeguards operational and effective?
- Focus: reliance on "digital nervous system," so protect the network

- The Incident Database: "Incoming fire has the right of way"
- Confidentiality Vs integrity for data: recognize integrity is a much larger domino
- The motivation of workers to end Apartheid was nothing short of extraordinary!

- Never have so few done so much in so little time (4 months start to finish)

Where did we poorly assess risk?

- Threat incidents did not stop, only increased in size, variety, and number (40,000+ by end of election)
- Threats and targets quickly change over time: political party, infrastructure, outsiders, wolf in the fold
- Sophistication of threat agents increases over time: playing "3D chess" with Zulu warriors; from anonymous bombs to personal bullets
- Unlikely motivations for threat agents (but understandable in retrospect)
- We focussed on threats to the political process, and forgot about "personal gain"
- "Up stream" suppliers (threats to food, security, transportation, communications, and electricity)
- People are the weakest link in the chain (personal character and their situation)
- A protest march by 200,000 angry people is an effective, highly motivated weapon of mass destruction
- Relying on technology: cell phones only last as long as the batteries do!
- NorthAm training does not prepare you for SouthAf life
- The election almost failed: Olympic athletes know they will win or lose by a fraction of an inch or second – we almost lost by underestimating the Olympian work effort that "democracy" demands, and only "pulled ahead" to win at the last second

Recommendations

- Stereotypes: training for "culture shock" and changes in personal security practices
- All potential motivations of threat agents need to be identified and used in the risk assessment
- Deterrence: high risk reduction from small incremental costs
- Safeguards are not safe: they only help to isolate threat incidents from having a wider impact. There is seldom a one-to-one correspondence between installing a particular safeguard and reducing/removing a particular vulnerability
- There are no technical fixes for management problems
- We tend to focus on the technical IT problems, but specific focus on solutions for people problems is vital
- Maybe Donn Parker was right: "… computer security is not primarily a technological subject. It is a subject of psychological and sociological behavior of people."
- ???